Telecom SIM Subscription Frauds: Global Policy Trends, Risk Assessments and Recommendations

Prof. Manish Gangwar, Dr. Shruti Mantri, Stephen Raveendra IPS, Kalmeshwar Shingenavar IPS
In an era defined by rapid technological advancements and interconnected digital networks, the telecommunications industry plays a pivotal role in shaping our global communication landscape. As the adoption of mobile devices and services continues to soar, the integrity and security of SIM subscriptions are paramount to ensuring trust and reliability in our interconnected world.

The phenomenon of SIM subscription fraud is a pressing issue that demands attention and concerted efforts from industry stakeholders, regulators, and law enforcement agencies. This report delves into the intricate dynamics of SIM subscription fraud, examining the various forms it takes, the vulnerabilities it exploits, and the far-reaching implications it has on individuals, businesses, and societal trust in telecommunications services.

Through in-depth analysis and case studies, this report sheds light on the evolving tactics used by fraudsters to manipulate and exploit vulnerabilities in SIM subscription processes. From identity theft and social engineering techniques to sophisticated cyber-attacks, the report aims to provide a comprehensive understanding of the complex nature of SIM subscription fraud and the challenges it poses to the security of telecommunications networks.

Furthermore, the report offers insights into best practices, industry guidelines, and technological solutions that can help mitigate the risks associated with SIM subscription fraud. By fostering collaboration, sharing knowledge, and implementing robust security measures, we can collectively enhance the resilience of mobile networks and safeguard the privacy and trust of users in an increasingly digital world.

I would like to extend my gratitude to the authors, teams from ISB, Centre of excellence, Cyber Bureau of Telangana police, contributors, researchers, and industry experts whose expertise and dedication have enriched this report. This document will serve as a beacon of knowledge and empowerment in our collective efforts to combat SIM subscription fraud and secure the foundations of our digital communications infrastructure.
Authors

**Professor Manish Gangwar**

Prof. Manish Gangwar is a distinguished faculty member and Executive Director of the Institute of Data Science at the Indian School of Business. Professor Gangwar has a Ph.D. in Management Sciences from the University of Texas at Dallas, an MS from University of Kentucky, and BE from the Indian Institute of Technology, Roorkee.

**Dr Shruti Mantri**

Dr. Shruti Mantri is a Chevening Cyber Security Fellow 2017 and is currently serving as Associate Director of the Institute of Data Science at the Indian School of Business. Dr. Shruti has Ph.D. in Computer Science from University Department of Computer Science, University of Mumbai, and Post Graduation from Cranfield University, United Kingdom.

**Mr Stephen Raveendra, IPS**

Mr. Stephen Raveendra is an IPS officer from 1999 batch, Telangana Cadre of the Indian Police Service. He has done his Post-Graduation in Zoology from Osmania University. He is currently serving as the Additional Director General of Police, Operations (GreyHounds and Octopus), Telangana.

**Mr Kalmeshwar Shingenavar, IPS**

Mr. Kalmeshwar Shingenavar is an IPS officer from 2012 batch, Telangana Cadre of the Indian Police Service. He has done his MBA specializing in Human Resources from Christ College, Bangalore. He is currently serving as the Commissioner of Police, Nizamabad District, Telangana.
Project Team

Indian School of Business

1. Mr. Kumara Guru, Sr. Director, External Relations
2. Mr. Sundeep Jammalamadaka, Associate Director, External Relations
3. Mrs. Varalakshmi Peketi, Manager, ISB Institute of Data Science
4. Ms. Shreshta Rikka, Data Analyst-cum-TA, ISB Institute of Data Science
5. Mrs. Selva Sundari, Data Analyst-cum-TA, ISB Institute of Data Science

Telangana Police Centre of Excellence for Cyber Security

1. Mrs. Riti Raj, IPS, Joint Director, Anti-Corruption Bureau
2. Mrs. K J Sneha, SI
3. Mr. M Venu, PC
4. Mr. G Ashok PC
5. Mr. CH Rajesh Khanna, PC
6. Mr. CH Sateesh Kumar, PC
# Table of Contents

Executive Summary 6  
Key Highlights 7  
Introduction 8  
SIM Subscription Fraud 12  
What is a Subscription Fraud or Identity Theft? 12  
Types of Subscription Frauds 12  
Problem Statement 12  
SIM Card Registration Policies prevalent in India and the World 13  
SIM Registration Process in India 14  
Vulnerabilities and Threats in the SIM Registration Process in India 18  
SIM Registration Policies Country-Wise 18  
Methodology 19  
Analysis of SIM Card Registration Policies 19  
Sampling 20  
Key Observations 21  
Countries with SIM Card Registration 21  
Countries without Mandatory SIM-Card Registration Laws 22  
Analysis 24  
Type of Subscriber Authentication and Validation 24  
Primary Identity Document 24  
Lack of Real-time Subscriber Authentication and Validation 25  
Ineffectiveness of OTP-based Authentication 27  
Irregularities on the part of the POS Agent 27  
Recommendations 28  
Authentication of Proof of Identity and Address documents 28  
Registration of Point of Sale (POS) agents 31  
Digitization of CAFs 32  
Prescribing a SIM Card Limit 32  
Conclusion 33  
References 34  
Glossary 35
Executive Summary

Effective identity verification solutions are the key to tackling telecommunication Subscriber Identity Module (SIM) card subscription frauds. Subscription fraud involves obtaining customer KYC details needed for signing up for new SIM cards or services with valid authorization but using the SIM cards for fraudulent activities. The effects of the damage done can be catastrophic in terms of financial fraud, poor customer experience, and damage to the brand. Telecom Service Providers (TSPs) face a massive challenge in this regard; they must overcome fraud while staying compliant with Department of Telecommunication (DOT) regulations. Most telecom service providers are currently using standard techniques for customer identity validation and verification, which are ineffective in detecting and controlling subscription fraud.

In this project, the researchers have:
(i) Assessed the risks in the current customer identity verification process,
(ii) Analysed the SIM registration policies in 160 countries,
(iii) Proposed multi-channel online identification validation methods, including knowledge-based validation, phone authentication, address validation, and one-time password use.

The recommendations proposed are based on a multi-layered risk-based approach that leverages intelligent analytics, predictive decision policies and knowledge-based authentication to enable real-time identity verification and regulatory compliance. The recommendations and report of the project outcome are submitted to Telangana Police.

The project was undertaken under the MOU with Telangana State Police Center of Excellence for Cyber Security.

Keywords: Subscription Fraud, Identity Theft, Identity Verification, Fabrication, Predictive Decision Policies, and Authentication.
The study presents an overview of the global and Indian mobile phone landscape, delving specifically into the growing threat of cybercrimes that often involve the use of fraudulent SIM cards and identity theft, making it challenging for law enforcement agencies to track and identify attackers.

The primary aim of the study is to investigate the prevalence of identity theft and subscription fraud in the telecommunications sector, scrutinising the security and authentication measures implemented by telecom service providers. Specifically, the focus is on evaluating vulnerabilities within SIM registration processes to identify areas that may be exploited by fraudsters.

64.5% of the consumers prefer the digital KYC process for SIM registration in India. Aadhar is the preferred proof of identity and proof of address but 89% of the consumer’s alternate number provided during sim registration is not linked to Aadhar.

The study extends its scope to conduct a comparative analysis of SIM registration policies across 160 countries worldwide. This broader perspective allows for the identification of best practices and the proposal of robust recommendations applicable globally.

The research highlights the inadequacies of OTP-based authentication, particularly the absence of a link between the alternate number and the legitimate subscriber, posing challenges in verifying its authenticity. Furthermore, it highlights irregularities in the practices of Point of Sale (POS) agents, such as the agents issuing SIM cards without proper verification and instances where cards are issued based on invalid or fake documents.

The report proposes a multi-layered risk-based approach, incorporating online identification and validation methods, and emphasises the importance of enhancing electronic identification and validation coupled with customer education to counter SIM subscription fraud.
Introduction

The reach of mobile phones continues to grow year upon year. With more than 7.26 billion mobile phone users in the world in July 2022, i.e. 91.54% of the world’s population, now owns a mobile phone, with almost 6.648 billion people in the world being smartphone users [1]. This means 83.72% of the world’s population owns a smartphone. This percentage is up considerably from 2016 when there were only 3.668 billion mobile phone users i.e. 49% of the global population.

According to GSMA (Groupe Speciale Mobile Association) real-time intelligence data, in July 2022 there were over 10.57 billion mobile connections worldwide, which surpasses the current world population of 7.93 billion as per the UN digital analyst estimates. This means there are 2.64 billion more mobile connections than people in the world. Over the last decade (2009-2019), access to mobile phones has grown rapidly, in terms of unique subscribers and total mobile connections. In the last 5 years (2017-2022), the number of global smartphone users has increased by 49.89% from 2017-2022 [1,2]. The biggest growth, in terms of unique mobile subscribers, was witnessed in Asia. It is estimated that the number of mobile users globally will reach 7.49 billion by 2025[1].

In India, the number of mobile telephone subscribers increased from 1,170.73 million at the end of May 2022 to 1,172.96 million at the end of June 2022[3], thereby showing a monthly growth rate of 0.19%. The number of mobile phone subscriptions increased from 647.81 million at the end of May 2022 to 649.09 million at the end of June 2022. The number of subscriptions in rural areas also increased from 522.92 million to 523.87 million during the same period.

Figure 1. Unique mobile subscribers as a percentage of the total population (2009)
Mobile penetration in 2019

- 51-70
- 71-90
- 91-100
- Inconclusive data or no data available

Figure 2. Unique mobile subscribers as a percentage of the total population (2019)

Mobile penetration in 2009

- 0-10
- 11-30
- 31-50
- 51-70
- 71-90
- 91-100
- Inconclusive data or no data available

Figure 3. Aggregate Mobile Connections as a proportion of the total population (2009)
Figure 4. Aggregate Mobile Connections as a Proportion of Total Population (2019)

Figure 5. Total Telephone Subscribers in India
Mobile phones have become a ubiquitous part of our lives. They do not just facilitate communication, but also enable access to several life-enhancing services especially banking and financial services. The increased dependency on technology makes its users vulnerable to cybercrimes. With threats becoming more sophisticated, the attacks on banking and financial sectors have considerably increased in the last 5 years. This disruption to the economy as a whole can be considered significant. In the first half of 2021, ransomware attacks in the banking sector increased by 1318%. In most financial frauds, cyber security attackers use fraudulent SIM cards or practice identity theft in order to hide their real identity. This makes it very difficult for law enforcement agencies to identify and track the attacker’s identity [3,4].

The purpose of this study is to identify the prevalence of identity theft or subscription fraud and determine if the telecom service providers are implementing the necessary security and authentication measures. The study presented in this report was meant to determine factors affecting subscription fraud and how the existing KYC-based (Know Your Customer) authentication is rendered ineffective when such frauds are committed. An analysis of the SIM registration processes across 160 countries reflects that the existing authentication processes in India are not sufficient. The study finds security flaws in the SIM registration processes that result in fraudsters being issued SIM cards, which they then use to commit banking and financial frauds. The findings of the study are the basis of the proposed recommendations that can curtail subscription and identity fraud.
What is a Subscription Fraud or Identity Theft?

As the number of mobile users and mobile services continues to increase, the potential for subscription fraud also increases. Subscription fraud occurs when a fraudster uses a stolen or synthetic identity to obtain telecom services and utilises them to commit cyber fraud. Fraudsters find ways to attract the attention of potential victims and entice them into revealing sensitive information. In doing so, they gain access to users’ details and use stolen, identities and credentials to purchase SIM cards. In certain situations, the users/customers provide sensitive information such as proof of identity (POI) and proof of address (POA) to fraudsters in exchange for financial benefits. This sensitive information is then used by fraudsters to purchase SIM cards. In the current study, researchers have identified the vulnerabilities in the Indian SIM registration processes and have recommended a framework for curtailing subscription fraud [5].

Types of Subscription Frauds

Subscription fraud can be categorized into two categories: First Party and Third-Party fraud.

• In First-party fraud, the customers own the identity but have no intention to pay for the services or devices they use.
• Third-party fraud entails the use of some form of impersonation or stolen identity, where stolen identity SIM cards are procured to commit future frauds [5].

Problem Statement

(i) Analyse the SIM registration framework in India, identify the vulnerabilities and threats, and propose recommendations.
(ii) Study and analyse the SIM registration policies across different countries in the world to propose robust recommendations.

Figure. 5 First-Party Fraud vs Third-Party Fraud.

First-Party Fraud vs. Third-Party Fraud

• Identity Theft
• Victim

• Financial Crime (Criminal Offence)

• Collectable
• No Victim
• Non-Financial Crime (Civil Offence)

Third Party: “not expecting to pay”

First-Party “won’t pay”

Bad Debt “can’t pay”
Post-paid mobile connections are usually linked to a fixed-term contract with the telecom service providers that helps in verifying the creditworthiness of customers in most countries. Prepaid (widely known as pay-as-you-go) SIM cards are easy to subscribe to and are the preferred option for many mobile users. 73% of all SIM cards globally are prepaid connections, with 79% of mobile users in Asia preferring prepaid SIM cards [11].

According to the GSMA Intelligence Mobile Penetration report people prefer prepaid SIM cards over post-paid cards. Mandatory SIM registration is a policy that requires users to provide proof of identity and proof of address, which includes information such as their name and national identification number, to get their prepaid SIM card registered or activated. SIM card registration is an important process that can be used to deter criminal activity such as SIM card subscription fraud and identity theft, thus preventing banking and financial frauds. SIM card registrations also help in authenticating subscribers so that they can access life-enhancing services such as mHealth, mEducation, financial products such as mobile money applications, and social protection.

As of January 2022, GSMA research found that the governments of 160 countries have made SIM card registration mandatory [3] and over 30 of these countries require biometrics e.g., fingerprints or a facial scan for registration of SIM card [1].

In some countries, governments require telecom service providers to capture photographs, fingerprints, and other biometric attributes of users at the time of registering users for SIM cards. 8% of countries require mobile operators to use biometric authentication processes when registering their users’ pre-paid SIM cards [3].
The SIM registration policies can be grouped into 3 different categories

(i) Capture and Store: The telecom service providers (TSPs) are required to capture and keep a record of subscribers’ details. The required information varies from one country’s jurisdiction to another globally. As of January 2020, about 73% of the countries (91 of the 125) mandate that SIM registration follow the capture and store approach [3].

(ii) Capture and Share: As of January 2020, 6% of the countries (10 out of 125) mandate that for SIM registration, telecom service providers (TSPs) should proactively capture and share the subscriber’s personal information with the government or regulator [3].

(iii) Capture and Validate: The telecom service providers (TSPs) are required and enabled to validate their customers’ identification credentials against a government central database, maintained by a government regulator or against a credential held by the customer such as a chip-based smart ID card. As of January 2020, 12% of the countries (24 out of 125), allowed telecom service providers to verify customer details against an approved government database or against credentials to facilitate the validation process [3].

SIM Registration Process in India

India’s telecom regulatory policies require a subscriber to register for both pre-paid and post-paid services. Subscriber details are captured and stored by telecom service providers. According to the Department of Telecommunication, there are four types of KYC document verification procedures:

(i) e-KYC
(ii) d-KYC
(iii) self-KYC
(iv) paper-KYC. [12-14]

Under each of these verification procedures, the stages of the registration process are:

(i) Application form with POA and POI
(ii) Validation
(iii) Subscriber Verification
(iv) Customer Signature
(v) Issue of SIM
(vi) Customer Verification
(vii) SIM Activation
(viii) Capture of Customer Details as Input
<table>
<thead>
<tr>
<th>Registration</th>
<th>Details</th>
</tr>
</thead>
</table>
| **Electronic (E)-KYC** | (i) Authorized Point of Sales (POS) of Licenses  
(ii) POS uses a mobile application for registration                                                                                                                                                 |
| **Digital (D)-KYC**   | POS uses a mobile application of the licensees for registration                                                                                                                                                                                                       |
| **Self-KYC**          | The customer uses a license application on the website and a mobile application                                                                                                                                                                                     |
| **Paper-KYC**         | The physical form is filled out by the customer and hard copies of the documents are submitted                                                                                                                                                                         |

<table>
<thead>
<tr>
<th>Proof of Identity</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Electronic (E)-KYC</strong></td>
<td>Aadhar Details</td>
</tr>
<tr>
<td><strong>Digital (D)-KYC</strong></td>
<td>Aadhar Card/d-Aadhar letter downloaded from the UIDAI website; Passport; Arms license; Driving license; Election Commission ID Card; Ration Card with a photo of the person undergoing verification*; CGHS/ECHS Card; Certificate of address with a photo, issued by a MP/MLA/Group-A Gazetted Officer on his/her letterhead; Certificate of address with a photo from a Govt. recognised educational institution <strong>; Certificate of photo identity issued by a village panchayat head or its equivalent authority</strong>*; Income Tax PAN Card; Photo Credit Card; Address card with a photo issued by Dept. Of Posts, Govt of India; Smart Card issued by the CSD, Defence/Paramilitary; Current passbook of a Post Office/any scheduled bank having a photo; Photo Identity Card****; Photo Identity Card issued by a Govt. recognised educational institution*****; Caste and Domicile Certificate with a photo; Pensioner Card with a photo; Freedom Fighter Card with a photo; Kisan Passbook with a photo; Sri Lankan Refugees Identity Card</td>
</tr>
<tr>
<td><strong>Self-KYC</strong></td>
<td>Aadhar Card/d-Aadhar letter downloaded from the UIDAI website; Passport; Arms license; Driving license; Election Commission ID Card; Ration Card with a photo of the person undergoing verification*; CGHS/ECHS Card; Certificate of address with a photo, issued by a MP/MLA/Group-A Gazetted Officer on his/her letterhead; Certificate of address with a photo from a Govt. recognised educational institution <strong>; Certificate of photo identity issued by a village panchayat head or its equivalent authority</strong>*; Income Tax PAN Card; Photo Credit Card; Address card with a photo issued by Dept. Of Posts, Govt of India; Smart Card issued by the CSD, Defence/Paramilitary; Current passbook of a Post Office/any scheduled bank having a photo; Photo Identity Card****; Photo Identity Card issued by a Govt. recognised educational institution*****; Caste and Domicile Certificate with a photo; Pensioner Card with a photo; Freedom Fighter Card with a photo; Kisan Passbook with a photo; Sri Lankan Refugees Identity Card</td>
</tr>
<tr>
<td><strong>Paper-KYC</strong></td>
<td>Aadhar Card/d-Aadhar letter downloaded from the UIDAI website; Passport; Arms license; Driving license; Election Commission ID Card; Ration Card with a photo of the person undergoing verification*; CGHS/ECHS Card; Certificate of address with a photo, issued by a MP/MLA/Group-A Gazetted Officer on his/her letterhead; Certificate of address with a photo from a Govt. recognised educational institution <strong>; Certificate of photo identity issued by a village panchayat head or its equivalent authority</strong>*; Income Tax PAN Card; Photo Credit Card; Address card with a photo issued by Dept. Of Posts, Govt of India; Smart Card issued by the CSD, Defence/Paramilitary; Current passbook of a Post Office/any scheduled bank having a photo; Photo Identity Card****; Photo Identity Card issued by a Govt. recognised educational institution*****; Caste and Domicile Certificate with a photo; Pensioner Card having a photo; Freedom Fighter Card with a photo; Kisan Passbook with a photo; Sri Lankan Refugees Identity Card</td>
</tr>
</tbody>
</table>
### PROOF OF ADDRESS

<table>
<thead>
<tr>
<th>Electronic (E)-KYC</th>
<th>Aadhar Details</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Digital (D)-KYC</strong></td>
<td>Aadhar Card/e-Aadhar letter downloaded from the UIDAI website; Passport; Arms License; Driving License*; Election Commission ID Card; Ration Card with a photo and address*; CGHS/ECHS Card; Certificate of address with a photo issued by a MP/MLA/Group-A Gazetted Officer on his/her letterhead; Certificate of address with a photo issued by a Govt. recognised educational institution**; Certificate of photo identity issued by village panchayat head or its equivalent authority***; Water bill*******; Telephone bill of a fixed line (not older than last three months); Electricity bill *******; Income Tax Assessment Order; Vehicle Registration Certificate; Registered Sale/Lease Agreement; Address card with a photo issued by Dept. Of Posts, Govt of India; Credit Card Statement; Caste and Domicile Certificate with address and a photo; Pensioner’s Card with address; Freedom Fighter Card with address; Kisan Passbook with address; Sri Lankan Refugees Identity Card</td>
</tr>
</tbody>
</table>

- **Self-KYC**
  - Aadhar Card/e-Aadhar letter downloaded from the UIDAI website; Passport; Arms License; Driving License*; Election Commission ID Card; Ration Card with a photo and address*; CGHS/ECHS Card; Certificate of address with a photo issued by a MP/MLA/Group-A Gazetted Officer on his/her letterhead; Certificate of address with a photo issued by a Govt. recognised educational institution**; Certificate of photo identity issued by village panchayat head or its equivalent authority***; Water bill*******; Telephone bill of a fixed line**; Electricity bill *******; Income Tax Assessment Order; Vehicle Registration Certificate; Registered Sale/Lease Agreement; Address card with a photo issued by Dept. Of Posts, Govt of India; Credit Card Statement; Caste and Domicile Certificate with address and a photo; Pensioner’s Card with address; Freedom Fighter Card with address; Kisan Passbook with address; Sri Lankan Refugees Identity Card |

- **Paper-KYC**
  - Aadhar Card/e-Aadhar letter downloaded from UIDAI website; Passport; Arms License; Driving License*; Election Commission ID Card; Ration Card with a photo and address*; CGHS/ECHS Card; Certificate of address with a photo issued by a MP/MLA/Group-A Gazetted Officer on his/her letterhead; Certificate of address with a photo issued by a Govt. recognised educational institution**; Certificate of photo identity issued by village panchayat head or its equivalent authority***; Water bill*******; Telephone bill of a fixed line**; Electricity bill *******; Income Tax Assessment Order; Vehicle Registration Certificate; Registered Sale/Lease Agreement; Address card with a photo issued by Dept. Of Posts, Govt of India; Credit Card Statement; Caste and Domicile Certificate with address and a photo; Pensioner’s Card with address; Freedom Fighter Card with address; Kisan Passbook with address; Sri Lankan Refugees Identity Card |

### VALIDATION

<table>
<thead>
<tr>
<th>Electronic (E)-KYC</th>
<th>Biometric/Aadhar details are used as a signature.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Digital (D)-KYC</td>
<td>OTP on the alternate number. (Self/ Relative/Known acquaintance)</td>
</tr>
<tr>
<td><strong>Self-KYC</strong></td>
<td>OTP sent to mobile linked to Aadhar</td>
</tr>
<tr>
<td><strong>Paper-KYC</strong></td>
<td>POI/POA documents submitted by customers</td>
</tr>
</tbody>
</table>

### SUBSCRIBER VERIFICATION

<table>
<thead>
<tr>
<th>Electronic (E)-KYC</th>
<th>Biometric</th>
</tr>
</thead>
<tbody>
<tr>
<td>Digital (D)-KYC</td>
<td>QR code on Identity Card, OR Information to be filled by Customer/POS</td>
</tr>
<tr>
<td><strong>Self-KYC</strong></td>
<td>Electronically verified POI/POA documents from UIDAI/Digi-locker</td>
</tr>
<tr>
<td><strong>Paper-KYC</strong></td>
<td>Self-attested copies of customer’s documents</td>
</tr>
</tbody>
</table>
CUSTOMER SIGNATURE

<table>
<thead>
<tr>
<th>Method</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Electronic (E)-KYC</td>
<td>Biometric Verification</td>
</tr>
<tr>
<td>Digital (D)-KYC</td>
<td>OTP sent on the alternate mobile number</td>
</tr>
<tr>
<td>Self-KYC</td>
<td>OTP sent on the alternate number</td>
</tr>
<tr>
<td>Paper-KYC</td>
<td>A physical signature of the customer</td>
</tr>
</tbody>
</table>

SIM ISSUED

<table>
<thead>
<tr>
<th>Method</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Electronic (E)-KYC</td>
<td>Inactive SIM is issued by the POS agent</td>
</tr>
<tr>
<td>Digital (D)-KYC</td>
<td>Inactive SIM is issued by the POS agent</td>
</tr>
<tr>
<td>Self-KYC</td>
<td>Inactive SIM is issued by the POS agent</td>
</tr>
<tr>
<td>Paper-KYC</td>
<td>Inactive SIM is issued by the POS agent</td>
</tr>
</tbody>
</table>

CUSTOMER VERIFICATION

<table>
<thead>
<tr>
<th>Method</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Electronic (E)-KYC</td>
<td>Licensee’s authorized representative</td>
</tr>
<tr>
<td>Digital (D)-KYC</td>
<td>Licensee’s authorized representative</td>
</tr>
<tr>
<td>Self-KYC</td>
<td>Licensee’s authorized representative</td>
</tr>
<tr>
<td>Paper-KYC</td>
<td>Licensee’s authorized representative</td>
</tr>
</tbody>
</table>

SIM ACTIVATION

<table>
<thead>
<tr>
<th>Method</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Electronic (E)-KYC</td>
<td>Licensee’s authorized representative</td>
</tr>
<tr>
<td>Digital (D)-KYC</td>
<td>Licensee’s authorized representative</td>
</tr>
<tr>
<td>Self-KYC</td>
<td>Licensee’s authorized representative</td>
</tr>
<tr>
<td>Paper-KYC</td>
<td>Licensee’s authorized representative</td>
</tr>
</tbody>
</table>

CUSTOMER DETAILS CAPTURED AS INPUT

<table>
<thead>
<tr>
<th>Method</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Electronic (E)-KYC</td>
<td>Live Photo with date, time, and location details</td>
</tr>
<tr>
<td></td>
<td>Demographic details attached to Aadhar number, fetched from the UIDAI database</td>
</tr>
<tr>
<td>Digital (D)-KYC</td>
<td>Live Photo with date, time, and location details</td>
</tr>
<tr>
<td></td>
<td>Demographic feature captured from QR code/filled by the customer</td>
</tr>
<tr>
<td>Self-KYC</td>
<td>Live Photo with date, time, and location details</td>
</tr>
<tr>
<td></td>
<td>Demographic details attached to Aadhar number, fetched from the UIDAI database</td>
</tr>
<tr>
<td>Paper-KYC</td>
<td>The hard copy of the documents submitted</td>
</tr>
<tr>
<td></td>
<td>Demographic data entered from POI/POA documents submitted by the customer</td>
</tr>
</tbody>
</table>

*Not applicable in Mumbai and Maharashtra Service
** For students only
*** For rural areas
**** For Central Govt./PSU or State Govt./PSU only
***** Issued by a State Govt. like Assam and other states
****** Should not be older than last three months
Vulnerabilities and Threats in the SIM Registration Process in India

During the consumer acquisition stage, a subscriber needs to provide proof of identity and proof of address. Identity verification and authentication is the key to the subscription process failures to detect forged ID or stolen ID while onboarding a customer. SIM-SWAP fraud is another major problem, whereby scammers use fake IDs to gain access to legitimate subscribers’ SIM cards. They then use this SIM to authenticate transactions with the real subscriber’s bank, make online purchases, and money transfers, and run up huge costs in the legitimate subscriber’s name. Telecommunication fraud resulting from a lack of real-time identity verification and authentication can result in fraudsters gaining access to SIM cards. Neural Technologies estimates the annual cost of identity fraud to the telecoms industry at €40 billion.

According to the Global CFCA Telecom Fraud, subscription or identity fraud constitutes 35% to 40% of all fraud experienced by the telecoms industry. There is a need to act fast to address the damages caused due to SIM Card fraud.

SIM Registration Policies Country-Wise

The mandatory SIM registration policy requires subscribers to provide personal information such as their name, national identification number, address, and proof of identity credentials to get a SIM card registered or activated. Existing users who fail to register their SIMs within the government-mandated time period can face network disconnection, resulting in loss of access to mobile services. As discussed earlier, around 160 countries in the world have mandatory SIM registration policies. In a few countries, telecom service providers are proactively introducing biometric authentication processes in anticipation of the government mandating this. While 160 countries, require individuals to prove their identity to register and/or activate their prepaid SIM cards, governments take different approaches to implementing SIM registration policies across different countries. The different approaches to collecting data, validating data, and storing data can be grouped into three categories: (i) Capture and Store (ii) Capture and Share (iii) Capture and Validate [11].

In countries where governments lack credible and reliable databases for mobile operators to conduct identity verification, the proof of identity varies. For example, in some countries, an attestation letter from the employer or a village elder, like in Nigeria, is an acceptable form of identification for SIM registration. However, such approaches are increasingly being phased out as they are perceived to be less robust and leave room for identity theft. An increasing number of governments, particularly those in Sub-Saharan Africa, are not only seeking to establish comprehensive digital identification systems as part of their digital transformation strategies, but are also seeking to achieve more robust identity verification when citizens and consumers attempt to access a suit of digital or electronic services (online or offline) [11].
Methodology

Analysis of SIM Card Registration Policies

In this study, we examined various factors to identify global regions where SIM-card registrations are more susceptible to cyber threat vectors. Additionally, we analysed SIM subscriber registration policies in India, comparing them to those in other countries. Some of the questions this study asks are:

(i) Whether biometrics are needed in the registration process;
(ii) Whether data is stored by providers or shared with government agencies;
(iii) What is (or is not) required for law enforcement to gain access to this data;
(iv) For how long is the data stored;
(v) Whether any data privacy legislation protects this information; and
(vi) Whether or not the countries have a mandatory IMEI database.[7]

The parameters that the study considers are:

(i) The requirement for registration
(ii) Capturing and storing data
(iii) Data privacy framework
(iv) Biometrics required in the registration process
(v) Data being stored by the telecom service providers or shared with the government agencies
(vi) Number of SIM cards allowed per person
(vii) Requirements for law enforcement agencies to gain access to the data
(viii) Penalties
(ix) Duration of data storage
(x) IMEI databases access country wise.

To conduct this study, we have used data from various sources [7]. We then conducted an in-depth analysis of each country’s laws to find out how the data collected during the SIM registration process was being used, stored and accessed.

In this study, we have used various sources ([1-4,7]) to find out whether SIM card registration is mandatory or not. We then did an in-depth study of each country’s laws to find out how this data is used, stored, and accessed. The examination involved assessing various parameters to identify regions where SIM card registrations are particularly susceptible to exploitation or security breaches. Every parameter was given a score and total scores were calculated. The total score was out of 18. Countries where no SIM card or IMEI registration was required automatically received a score of 18. We found that in countries with scores of 15 and above, SIM registration policies faced major risks and could be exploited by attackers for identity theft/subscription fraud.

Registration Requirement

1. Registration required = No (1 point), Yes (0 points), Optional (0.5 points)
2. Capture and Store = 1 point
3. Capture and Share = 2 points
4. Capture and Validate = 0 points

Data Privacy Framework

1. Yes (0 points)
2. No (1 point)

Biometric Information

1. Fingerprints and/or facial patterns (0 points)
2. Fingerprints used for limited groups (i.e., those without ID (1 point))
3. In progress (2 points)
4. No Biometric (3 points)
SIM Card Limit
1. 5 or less (0 points)
2. 6 to 10 (1 point)
3. Over 10 or other restrictions (2 points)
4. No limit (3 points)

Law Enforcement Access
1. Severe interception capabilities (2 points)
2. Without warrant (1 point)
3. With warrant (0 points)

Penalties
1. Subscriber prison sentences and/or penalties (0 points)
2. Subscriber penalties/fines (1 point)
3. Subscriber deactivation (2 points)

Data Storage
1. 6 or more years (0 points)
2. 4 to 5 years (1 point)
3. 2 to 3 years (2 points)
4. Up to 1 year (3 points)
5. Length of contract and up to six months after (4 points)

IMEI Registration
1. Mandatory (0 points)
2. Not Mandatory (1 point)

Sampling
The subscriber data across all the telecom service providers is stored by the way of customer acquisition forms (CAFs). These forms are made available to law enforcement agencies in a portable document format (PDF) after a criminal case is filed and registered. 1600 CAFs across different service providers were obtained by the Cyberabad Police Commissionerate from different police stations across Hyderabad and Telangana. For real-time analysis, the data from all Customer Acquisition Forms (CAFs) in PDF format was extracted into an Excel sheet using a Python program.
Countries with SIM Card Registration

India’s telecom regulatory policies require a subscriber to register for both pre-paid and post-paid services; subscriber details are captured and stored by telecom service providers. There are three types of KYC document verification procedures: (i) e-KYC (ii) d-KYC (iii) self-KYC. In India, a biometric check is compulsory only for e-KYC and self-KYC processes, both of which utilise Aadhar numbers for the verification of subscriber details. While registering a new SIM card, a live photograph is captured in e-KYC and d-KYC as per the process of the Department of Telecommunication. Telecom service providers capture and validate data against a central database for the e-KYC SIM card registration process. For the d-KYC and paper-KYC registration process, the data is captured and stored. For law enforcement officers, information is made available as and when needed based on the criminal complaint filed by the victim. Currently, every subscriber can subscribe to a maximum of 9 SIM cards with the same or across different telecom service providers in the same state or separate states.

The countries that currently have biometric registration laws are Bahrain, Bangladesh, Belarus, Benin, China, Ghana, Jordan, Lesotho, Mexico, Nigeria, Oman, Pakistan, Peru, Saudi Arabia, Singapore, Tajikistan, Tanzania, Thailand, Uganda, United Arab Emirates, Venezuela, and Zambia. Countries such as Ethiopia, Indonesia, Japan, Lebanon, Liberia, Jordan, Lebanon, Liberia, North Korea, and Russia are in the planning stage of implementing biometric authentication. In Mozambique, subscribers can provide their fingerprints if they don’t have adequate ID (Figure 7).

Key Observations

In 90 countries, where prepaid SIM registration is mandatory, telecom service providers capture and store their customer’s identification credentials. Out of 90 countries, 10 countries capture biometric data of the customers such as facial scans, fingerprints, or both. Jordan and Myanmar are two countries that capture biometric data such as fingerprints and facial scans but there is no data privacy framework or policy, thereby increasing the risk of a data breach.

Telecom service providers in 24 countries, capture and validate customers’ credentials with a central government database. Out of 24 countries, 11 countries capture biometric data of the customers such as facial scans, fingerprints, or both. Pakistan and Tanzania capture and validate the customer’s biometric data but have no data privacy framework. Pakistan stores the data for one year increasing the risk of a data breach.

In 10 countries, telecom service providers capture and share customer data with the government. Benin, Lesotho, and Nigeria capture and share biometric data such as fingerprints. Sierra is the only country that captures and shares the data and has no data privacy framework in existence.

Bangladesh, India, and Saudi Arabia with a score of 7, capture and validate the customer details against the government database and penalize the subscriber with deactivation or fine if they fail to comply with the SIM registration framework.

In China, Myanmar, Nigeria, and Singapore, individuals registering a new phone number are required to submit to a facial scan. In all other countries where biometrics are not implemented, a photo ID is mandatory for the registration process.
In 79 countries there is no limit on the SIM cards that can be allocated to a single subscriber. South Korea is the only country that allows 1 SIM card per person. Myanmar allows 2 SIM cards per person. Pakistan, Sri Lanka, and the Gambia allow a maximum of 5 SIM cards per subscriber. Most countries allow the subscriber to procure more than 5 or unlimited access to SIM cards.

16 countries store the IMEI number of the device, and the SIM cards are activated only for that registered and verified IMEI number.

Countries without Mandatory SIM-Card Registration Laws

Currently, 31 countries do not have a mandatory SIM card registration policy in place. These countries are: Bosnia and Herzegovina, Canada, Cabo Verde, Comoros, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, Iceland, Ireland, Israel, Kiribati, Latvia, Liechtenstein, Lithuania, Maldives, Malta, Marshall Islands, Micronesia, Moldova, Namibia, the Netherlands, New Zealand, Nicaragua, the Philippines, Portugal, Romania, Serbia, Slovenia, Sweden, the United Kingdom, the United States, and Vanuatu.
Figure 7. SIM Card Registration Laws Country-wise

Figure 8. Types of SIM-Card Registration
The primary objective of the study was to understand the extent of the adoption of SIM registration policy in India and to identify the gaps in the existing processes of subscriber authentication and validation.

**Type of Subscriber Authentication and Validation**

The data extracted was analysed for the following telecom service providers:

(i) Vodafone  
(ii) Jio  
(iii) Idea  
(iv) Airtel  
(v) BSNL

Three different types of customer verification process were used:

(i) e-KYC  
(ii) d-KYC  
(iii) p-KYC

It was found that around 90% of subscribers preferred digital KYC as an identity verification process as compared to a biometric verification system.

**Primary Identity Document**

Aadhar is the primary national identity document used as proof of identity and proof of address (Table 6.2), followed by a Voter-ID card in the digital KYC. Around 90% of the valid Aadhar cards used in digital KYC were found to be not linked to the Aadhar cards. SMS-based OTP-based authentication was rendered ineffective as the alternate number used for OTP authentication was not linked to the Aadhar (Table 6.3) and belonged to a third party, whose identity was unknown.

**Table 6.1 Registration Process TSP-wise**

<table>
<thead>
<tr>
<th>Telecom Service Provider</th>
<th>Number of CAFs</th>
<th>e-KYC</th>
<th>d-KYC</th>
<th>p-KYC</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1412</td>
<td>496</td>
<td>911</td>
<td>5</td>
</tr>
</tbody>
</table>

**Table 6.2 National Identity used for Registration Process**

<table>
<thead>
<tr>
<th>Telecom Service Provider</th>
<th>SIM Registration Process</th>
<th>Aadhar</th>
<th>Voter Id Card</th>
<th>Driving License</th>
</tr>
</thead>
<tbody>
<tr>
<td>e-KYC</td>
<td>496</td>
<td>00</td>
<td>00</td>
<td>00</td>
</tr>
<tr>
<td>d-KYC</td>
<td>836(91.76%)</td>
<td>55(6%)</td>
<td>20(2.19%)</td>
<td></td>
</tr>
</tbody>
</table>

**Table 6.3 Aadhar Card Analysis**

<table>
<thead>
<tr>
<th>Telecom Service Provider</th>
<th>SIM Registration Process</th>
<th>Aadhar</th>
<th>Valid</th>
<th>Not Valid</th>
<th>Alternate number not matching with Aadhar</th>
<th>Alternate Numbers matching with Aadhar</th>
</tr>
</thead>
<tbody>
<tr>
<td>d-KYC</td>
<td>836</td>
<td>736</td>
<td>100</td>
<td>745 (89.11%)</td>
<td>214</td>
<td></td>
</tr>
</tbody>
</table>
Lack of Real-time Subscriber Authentication and Validation

**e-KYC**
In the e-KYC process, biometrics serve as the primary authentication method. However, for subscribers registered before 2021, inconsistencies arise in the profile photographs retrieved from UIDAI/Aadhar-linked photographs, often not aligning with the current-day images of the subscribers. There is no verification of the current-day profile photograph with the photograph retrieved from UIDAI. For subscribers registered after 2021, the profile photograph retrieved from UIDAI does not match the current day photograph in many cases. The current-day photograph is that of an adult and the photograph retrieved from UIDAI is of a minor under 18. This vulnerability is exploited by fraudsters to carry out identity theft and subscription fraud attacks.

**Digital-KYC:**
In the Digital-KYC process, subscribers can use various documents, including Voter-ID cards, PAN cards, passports, and Aadhar cards for proof of identity and address. However, the Aadhar document is the preferred primary national identity document, with 89% of people opting for Aadhar cards as proof of identity and address. In the current process, the POS agent captures the live photograph of the subscriber and the live photograph of the national identity document. But there is no real-time verification of the photograph on the Aadhar card/Voter-ID card and the live photograph captured, resulting in instances where even though there is a mismatch between the two photographs, a SIM card is being issued to the subscriber. The POS agent also does not verify the authenticity and validity of the proof of identity document with the competent authority. The same is also not verified by the telecom service providers’ authorized representatives. The fraudsters exploit the lack of real-time verification vulnerability to carry out identity theft or a subscription fraud attack to procure SIM cards for illegal activities.

**Paper-KYC:**
In a Paper-KYC, the subscribers provide hard copies of their documents along with a passport-size photograph. The POS agent does not perform real-time verification of documents provided with the respective competent authority such as UIDAI/mparivahan, etc. for verifying subscriber details nor do they verify the real-time photo with the photo provided. Due to the lack of real-time verification and authentication processes, the fraudsters can compromise the system and get a SIM card issued.
Figure 9. Lack of Real-Time Validation in E-KYC Authentication Process

Figure 10A. Profile Photograph of a Minor in e-KYC Authentication Form

Figure 10B. Profile Photograph of a Minor in CAF Form.
Figure 11. Invalid Aadhar Document used for Subscriber Registration

Ineffectiveness of OTP-based Authentication

In the current system, as prescribed by the Department of Telecommunication (DOT), the alternate number can belong to a oneself, a relative or a known person. In most of the CAFs, the alternate number does not belong to the customer requesting a new SIM nor it is linked with the respective national identity card such as an Aadhar card/telephone registered with mAadhar, mParivahan or the Voter-ID card. Due to this, the fraudsters are able to give a third party’s number as an alternate number for OTP authentication thereby making it extremely challenging to verify the authenticity of the alternate number. The CAFs have no details regarding the owners of the alternate numbers, thus making it extremely challenging to trace the alternate number owners or establish linkages between the owner of the alternate number and the fraudsters in the event of a fraud.

Irregularities on the part of the POS Agent

Point of Sale (POS) agents are crucial in verifying subscribers’ proof of identity and proof of address documents. Upon analysing Customer Acquisition Forms (CAFs), numerous irregularities were identified in the practices of Service Providers’ Point of Sale (POS) agents in issuing new mobile connections. SIM cards were issued without verifying the proof of identity and proof of address. For instance, SIM cards were issued even if the profile photograph did not match the current-day photograph. In some cases, the SIM cards were issued on school/college ID cards. There were also instances where SIM cards were issued on fake/invalid documents. Such illegally acquired SIMs are also used in cyber crimes such as KYC frauds and for sending phishing SMSs to customers. It is observed that the Point of Sale (POS) agents/retailers/distributors are one of the major contributors to the fact of SIMs being used in illegal activities.
**Recommendations**

The risk analysis of the existing processes exposed the vulnerabilities that are exploited by attackers to design and execute subscription fraud. There is an imperative to find a solution that provides different online identification and validation methods, including knowledge-based validation, phone authentication, address validation, one-time password use, and use of common username across multiple telecom service providers to enhance electronic identification and trust. In the current study, we have performed a risk assessment of the existing e-KYC, d-KYC and p-KYC processes; identified the threat vectors and vulnerabilities and proposed solutions for strengthening the process as outlined below.

**Authentication of Proof of Identity and Address documents**

<table>
<thead>
<tr>
<th>Department of Telecommunication (DOT) Circular</th>
<th>Process</th>
<th>Threats</th>
<th>Vulnerabilities</th>
<th>Recommendations</th>
<th>Stakeholders</th>
</tr>
</thead>
</table>
| e-KYC 800-12/2019-AS. II dated 21.09.2001    | Authentication: The live photograph of the customer is taken by the POS agent with the date and time stamp. | Authentication Failure: The photograph retrieved from UIDAI does not match the current-day profile photograph of the subscriber. | • The POS agent captures the live photograph of the customer, but the live photograph is not validated with the UIDAI profile photograph.  
• The TSP application does not have the capability to verify the live photograph and the UIDAI photograph. | The TSP application should perform real-time verification of customer identity of proof and address. | DOT TSP |

| e-KYC 800-21/2015-AS. II dated 7.12.2021    | Authentication: Prior to 2021 | Authentication Failure: For SIMs procured on or before 2021 using e-KYC, only the profile photograph is retrieved from UIDAI. The live photograph is missing. | The live photograph of the subscriber is not verified with the profile photograph retrieved from UIDAI. | All the CAFs with e-KYC before 2021 should have a live photograph and the same needs to be verified with the photograph retrieved from the Aadhar database. The same needs to be verified by TSP systems and digitally signed by TSP. | DOT TSP |

<p>|                         | Identity Theft: The CAF details of the number linked with Aadhaar are not captured in the current CAF. | The customer details of the alternate number linked with Aadhar are not linked to the new number. | The CAF of the phone number linked with Aadhaar which is being used as a POI document to issue the new number and the CAF of the number of the new number should be linked. | | |</p>
<table>
<thead>
<tr>
<th>Department of Telecommunication (DOT) Circular</th>
<th>Process</th>
<th>Threats</th>
<th>Vulnerabilities</th>
<th>Recommendations</th>
<th>Stakeholders</th>
</tr>
</thead>
</table>
| d-KYC 800-26/2016-AS-II dated 03.04.2019      | Authentication | Fabrication: The live photograph does not match the profile photograph on the Aadhar card. | The POS captures the live photograph of the customer but does not verify with the photograph on Aadhar/alternate ID-Proof | • If the subscriber uses Aadhar as a POI/POA document, the TSP system should validate the live photograph with the UIDAI details.  
• The TSP application should be able to capture the photograph from the POI/POA document and verify it with a live photograph. | DOT TSP |
|                                               | ID proof has the photograph of a minor, and the live photograph is that of an adult. | Real-time validation of identity is not done. | The photograph on Aadhar or ID needs to be updated every 5 years. | UIDAI |
|                                               | Identity Theft: The alternate number used for authentication is not linked with the Aadhar number. | The subscriber identity of the alternate number used for authentication is not validated. | The CAF of the phone number linked with Aadhaar which is being used as a POI document to issue the new number should be linked with the CAF of the new number. | TSP DOT UIDAI |
|                                               | Invalid/Fake Documents: Coloured and laminated photocopies of Aadhar Cards are used. Hence the QR code does not work to retrieve data connected with the Aadhar number. | Xerox and laminated Aadhar are used and accepted by POS and TSP. | • The TSP application should scan the QR code to verify the original document of POI/POA.  
• Only documents with valid QR codes should be accepted. | UIDAI TSP POS |
<p>|                                               | Real-time verification of subscriber details is missing. | The TSP system does not verify the subscriber details. | The TSP applications need to verify the subscriber details in real time. | TSP UIDAI Election Commission Transport Authority |</p>
<table>
<thead>
<tr>
<th>Department of Telecommunication (DOT) Circular</th>
<th>Process</th>
<th>Threats</th>
<th>Vulnerabilities</th>
<th>Recommendations</th>
<th>Stakeholders</th>
</tr>
</thead>
</table>
| d-KYC                                         |         |         | Distorted or blurry profile photographs are used on Voter-ID cards. | Documents with distorted or blurry images are accepted. | Only original documents in a readable format are to be accepted by the TSP application.  
  • If an Aadhar card is used as POI/POA only the Aadhar details are to be verified in real-time by querying the UIDAI database.  
  • Only e-Driving license issued by mParivahan to be used as POI/POA. |
| Authentication                                 |         |         | The clarity of the POI/POA document is missing. | Voter-ID cards and driving licenses are not being verified with the regulatory authority. | Voter-ID cards and driving licenses to be verified in real time.  
  DOT  
  TSP  
  mParivahan  
  Election commission |
| F-KYC                                         |         |         | Authentication Failure | Physical documents are not verified with the respective authority. | The TSP application should scan the physical documents and perform real-time verification to verify the subscriber’s authenticity. For example, the Aadhar card should be verified with UIDAI before SIM activation.  
  DOT  
  TSP  
  POS |
|                                               |         |         | CAFs are scanned and stored in the form of images and hence data cannot be retrieved. | CAFs need to be stored in a retrievable format | DOT  
  TSP |
## Registration of Point of Sale (POS) agents

<table>
<thead>
<tr>
<th>Current Eligibility for POS</th>
<th>Process</th>
<th>Threats</th>
<th>Vulnerabilities</th>
</tr>
</thead>
</table>
| Currently, there is no eligibility criteria for authorized POS | Real-time verification of POS agent missing | (i) Basic Education Qualification Criteria  
(ii) License for POS - Mandatory registration of POS with a DOT body/wing; upon which a license/permit may be granted to operate/function as POS agent. If the proposed POS agent meets the prescribed eligibility criteria, the application for obtaining a POS license/permit shall be routed through the TSP on behalf of the POS agent.  
(iii) Background police verification with respect to criminal antecedents. | TSP  
DOT |

### Training

| Training | Compromising authentication and integrity of the verification processes due to lack of knowledge of cybercrimes and SIM registration process. | (i) The POS agent shall be trained by the TSP for issuance of SIM as mandated by DOT, on the various processes (e-KYC, d-KYC, self-KYC and paper-KYC).  
(ii) Training to be prescribed by DOT. | DOT  
TSP |

### Licenses

| License required to become a POS agent | No real-time authentication of POS agent. | (i) The DOT may prescribe a validity period of 2 to 3 years for the license/permit. After the expiry of the validity period, the POS agent may seek renewal from time to time.  
(ii) The POS agent shall give a deposit amount to secure the permit and in case of any wrongdoing, the deposit amount shall be forfeited. | |

### Operational

| Biometric Access to TSP application | The TSP application is compromised by social engineering attacks leading to username/password being shared with a third party or the outsourcing of work of SIM registration resulting in a compromise in the authentication process as well as integrity of other processes. | (i) Biometric Authentication to Access TSP App.  
(ii) The access to the TSP’s mobile/laptop application shall not only be through ID and password but must also include biometric authentication of the POS agent. This would prevent misuse of the App and device by other third parties. | |
## Digitization of CAFs

<table>
<thead>
<tr>
<th>Subscriber for Data</th>
<th>Current Challenges</th>
<th>Recommendations</th>
<th>Stakeholders</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lack of real-time</td>
<td>Lack of real-time verification of subscriber data on a criminal complaint being</td>
<td>Digitization of CAFs to facilitate verification of the fraudulent SIM card details on registering a complaint.</td>
<td>TSP</td>
</tr>
<tr>
<td>verification of</td>
<td>registered.</td>
<td></td>
<td>DOT</td>
</tr>
<tr>
<td>subscriber data</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>on a criminal</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>complaint being</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>registered.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

## Prescribing a SIM Card Limit

<table>
<thead>
<tr>
<th>SIM Card Limit</th>
<th>Current Challenges</th>
<th>Recommendations</th>
<th>Stakeholders</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum 9 sim cards</td>
<td>Details of alternate numbers not verified during the registration.</td>
<td>Verification of maximum limit of SIM cards issued to a subscriber on issuing a new SIM card.</td>
<td>TSP</td>
</tr>
<tr>
<td>allowed per person</td>
<td></td>
<td></td>
<td>DOT</td>
</tr>
</tbody>
</table>
SIM card subscription fraud is a pervasive issue within the telecommunications industry. It involves malicious actors who acquire customer KYC (Know Your Customer) details to fraudulently obtain new SIM cards or services, all while seemingly complying with valid authorization procedures. These fraudsters subsequently employ these SIM cards for nefarious activities, leading to dire consequences such as financial fraud, compromised customer experiences, and damage to the brand's reputation. This predicament poses a significant challenge for telecom service providers, who must navigate the delicate balance between countering fraud and adhering to Department of Telecommunication (DOT) regulations.

Preventing SIM card subscription fraud is paramount for telecommunications companies to safeguard their customers and maintain the integrity of their services. Some key strategies identified to mitigate this threat are:

- **Enhanced Identity Verification:** Strengthening customer identity verification by implementing more robust processes for authentication of proof of identity and proof of address documents.
- **Registration of Point of Sale Agents:** Ensuring the registration of POS agents and training them to conduct customer verifications in all forms: e-KYC, d-KYC, self-KYC and paper-KYC.
- **Digitisation of CAFs:** Digitising CAFs to facilitate verification of the fraudulent SIM card details when a complaint is registered.
- **Verification of maximum limit of SIM cards:** Prescribing a limit for the maximum number of SIM cards that can be issued to a subscriber and verifying previous SIM cards while issuing a new SIM card.

Last but not the least, it is imperative to educate customers about the risks of sharing personal information and the importance of reporting lost or stolen SIM cards promptly.

Preventing SIM card subscription fraud requires a combination of technological advancements, vigilance, and regulatory cooperation. By implementing these measures, telecom service providers can significantly reduce the risk of SIM card fraud, protecting their customers and their reputation.
References


[3] GSMA Intelligence Mobile Penetration (unique subscribers as a percentage of the total population) Q3 2007 and 2017, accessed on 20/07/2022


[14] 800-26/2016-AS.II, Dated 03.04.2019, Government of India, Ministry of Communications, Department of Telecommunications
Glossary

CAF: Customer Acquisition Form
DOT: Department of Telecommunication
GSMA: Groupe Speciale Mobile Association
ID: Identity Document
IMEI: International Mobile Equipment Identity
KYC: Know Your Customer
mAadhaar: Official mobile application developed by UIDAI
mEducation: Educational Initiatives supported by mobile devices
mHealth: Practice of medicine and public health supported by mobile devices
mParivahan: Official mobile application for various vehicle related services at Road Transport Offices level
MOU: Memorandum Of Understanding
OTP: One Time Password
PDF: Portable Document Format
POA: Proof of Address
POI: Proof of Identity
POS: Point of Sale
QR code: Quick Response Code
SIM: Subscriber Identity Module
SMS: Short Message Service
TSP: Telecom Service Provider
UIDAI: Unique Identification Authority of India
Indian School of Business

Hyderabad Campus: Gachibowli, Hyderabad - 500 111, Telangana, India.
Mohali Campus: Knowledge City, Sector 81, SAS Nagar, Mohali - 140 306, Punjab, India.